AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of determining network penetration, the method comprising the computer-implemented steps of:

representing a possible travel of a packet in a network based on topology data and on security policy data; ~~and,~~

wherein the step of representing comprises:

checking an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet;

if the inbound ACL permits ingress of the packet, checking one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted;

for each of the one or more possible outbound interfaces on which the egress of the packet is permitted, repeating the checking steps with respect to each neighbor network device that is connected to each of the one or more possible outbound interfaces;

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing;

wherein the steps of the method are performed by one or more computer systems.

2. (Original) A method as recited in Claim 1, wherein the security policy data comprises one or more access control lists of one or more network devices in the

network.

3. (Original) A method as recited in Claim 1, further comprising the step of receiving packet parameters.

4. (Currently Amended) A method as recited in Claim 3, wherein the packet parameters comprise ~~an~~ the network entry point where the packet enters the network.

5. (Original) A method as recited in Claim 3, wherein the packet parameters comprise a destination address.

6. (Original) A method as recited in Claim 1, wherein the topology data is received as input related to a user interface.

7. (Original) A method as recited in Claim 1, wherein the security policy data is based on access control lists associated with input received in a user interface.

8. (Original) A method as recited in Claim 1, further comprising determining a maximum penetration point.

9. (Currently Amended) A method as recited in Claim 1, wherein the step of representing comprises accessing the security policy data and the topology data related to a neighbor network device for which it has been determined that the packet could reach.

10. (Currently Amended) A method as recited in Claim 1, wherein the step of representing

comprises determining whether ingress is allowed to a neighbor network device for which it has been determined that the inbound interface could be reached by the packet.

11. (Currently Amended) A method as recited in Claim 1, wherein the step of representing comprises determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet could reach.

12. (Original) A method as recited in Claim 1, wherein the step of representing comprises determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

13. (Original) A method as recited in Claim 12, wherein the step of representing comprises recursively applying the step of determining whether there are any outbound interfaces.

14. (Canceled)

15. (Original) A method as recited in claim 1 further comprising receiving packet parameters specifying information corresponding to a plurality of packets.

16. (Currently Amended) A method as recited in claim 1 wherein the step of representing comprises:

~~at~~ for a neighbor network device ~~that~~ for which it is determined that the packet could reach, determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress of the packet is permitted based on the static routing table.

17. (Currently Amended) The method of claim 16, further comprising not considering ~~permitting egress through~~ any outbound interface through which egress of the packet is permitted by the static routing table[[,] but is not permitted by an access control list associated with the security policy data.

18. (Currently Amended) A method as recited in claim 1 wherein the step of representing comprises:

~~at~~ for a neighbor network device for which it is determined that the packet could reach, determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface of the neighbor network device, representing an egress by the packet as part of the representing of the travel of the packet.

19. (Original) A method as recited in claim 1, further comprises receiving packet parameters that support transmission control protocol flags.

20. (Original) A method as recited in claim 1, wherein the results comprise a graphical display of at least allowed paths of the packet.

21. (Original) A method as recited in claim 19, wherein the graphical display also includes at least a mapping of network devices and connections between the network

devices.

22. (Currently Amended) A method of determining potential penetration of a packet into a network, the method comprising the computer-implemented steps of:

receiving network topology data;

receiving first information defining a packet flow comprising a source address;

receiving second information defining a first network device, comprising a network address and an ingress interface identifier for an ingress interface;

determining whether the ingress interface of the first network device allows the packet flow to enter the first network device, based on a first access control list associated with the ingress interface;

determining one or more egress interfaces of the first network device that allow egress of the packet flow, based on one or more second access control lists associated with the one or more egress interfaces;

based on the network topology data, determining one or more second network devices that are coupled to the one or more egress interfaces; and

recursively performing the determining steps for each of the one or more second network devices;

wherein the steps of the method are performed by one or more computer systems.

23. (Original) A method as recited in Claim 22, further comprising the steps of determining if a static routing table is present, and wherein the step of determining the one or more egress interfaces is performed based on the static routing table.

24. (Currently Amended) The method of claim 23, further comprising not ~~permitting egress through~~ considering an outbound interface through which egress of the packet flow is permitted by the static routing table[[,]] but is not permitted by the one or more second access control lists.

25. (Currently Amended) A method of determining network penetration, the method comprising the computer-implemented steps of:

representing a travel of a packet in a network based on topology data and on security policy data including at least the steps of:

defining a packet by at least specifying a source address, an entry port, and a destination port;

starting a loop for a current network device;

accessing access control list (ACL) data stored in an ACL database and the topology data stored in a topology database;

deciding whether an ingress interface of a current network device allows entry into the current network device, wherein:

if the entry is not permitted, then terminating the loop for the current network device,

if the entry is permitted, then performing the steps of:

checking one or more outbound ACLs for each outbound interface of the current network device to determine one or more possible outbound interfaces on which egress of the packet is permitted;

continuing the loop;

determining if a static routing table is present, wherein:

if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and

if the static routing table is not present, then determining that ~~allowing~~ outbound traffic is allowed to exit through all outbound interfaces;

based on the topology data, determining if there are any neighboring network devices that are connected to the one or more possible outbound interfaces on which the egress of the packet is permitted from the current network device, wherein:

if there are not any neighboring network devices, then returning an indication of the current network device ~~is returned~~ as a maximum penetration point as at least part of results of the step of representing, and terminating the loop ~~is terminated~~;

if there is at least one neighboring network device, then continuing the loop; ~~continues~~

determining whether or not there are any remaining possible outbound interfaces for which results of a possible egress of the packet have not been determined, wherein:

if there are no more remaining possible outbound interfaces, then terminating the loop ~~is terminated~~,

if there are more remaining interfaces, then setting the current network device ~~is set~~ to ~~the~~ a neighboring network device that corresponds to ~~corresponding~~ one of the remaining possible outbound

interfaces, and

if the loop has not been terminated for the current network device, then

restarting the loop for the current network device;

wherein the steps of the method are performed by one or more computer systems.

26. (Currently Amended) An ~~system~~ apparatus for determining penetration into a network, the ~~system~~ apparatus comprising:

one or more processors;

a topology database storing topology information about the ~~database~~ network;

an Access Control List (ACL) database storing ACL information related to the network;

a computer-readable storage medium ~~carrying~~ storing one or more sequences of instructions that comprise instructions for displaying a penetration Graphical User Interface (GUI) including at least:

input fields having at least:

a topology information input field,

an ACL input field,

a source address input field for entering at least a source address of a packet,

an entry point ~~entry~~ field for entering at least [[a]] one entry point to the network for the packet, and

a destination input field for entering at least a destination address for the packet[[,]]; and

output penetration information fields ~~including at least~~ for a graphical output including: ~~at least a representation of~~

network devices of the network,

connections between the network device corresponding to the topology data,

at least one entry point to the network,

paths the packet is allowed to follow based on the topology data and the ACL data,

at least one maximum penetration point; and

a penetration module ~~that~~ configured to:

accesses the topology database[[,]];

accesses the ACL database[[,]];

receives input corresponding to the input fields[[,]];

check an inbound ACL of an interface of a network device specified by the input in the entry point field;

if the inbound ACL permits ingress of the packet, check one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted; and

produces the output penetration information for display in the penetration GUI.

27. (Currently Amended) An ~~system~~ apparatus for determining network penetration, the ~~system~~ apparatus comprising:

one or more processors, and a computer-readable storage medium ~~carrying~~ storing one or more sequences of instructions that comprise instructions which, when executed by the one or more processors, cause ~~for causing~~ the one or more

processors to ~~carry out a method comprising~~ perform the steps of:

representing a possible travel of a packet in a network based on topology data and on security policy data; ~~and,~~

wherein the step of representing comprises:

checking an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet;

if the inbound ACL permits ingress of the packet, checking one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted;

for each of the one or more possible outbound interfaces on which the egress of the packet is permitted, repeating the checking steps with respect to each neighbor network device that is connected to each of the one or more possible outbound interfaces;

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing.

28. (Currently Amended) An ~~system~~ apparatus as recited in Claim ~~26~~ 27, wherein the security policy data comprises one or more access control lists stored on one or more network devices in the network.

29. (Currently Amended) An ~~system~~ apparatus as recited in Claim ~~26~~ 27, ~~the method further comprises~~ wherein the one or more sequences of instructions further comprise

instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving packet parameters.

30. (Currently Amended) An ~~system~~ apparatus as recited in Claim 29, wherein the packet parameters comprise an entry point where the packet enters the network.

31. (Currently Amended) An ~~system~~ apparatus as recited in Claim 29, wherein the packet parameters comprise a destination address.

32. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the topology data is based on input related to a user interface.

33. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the security policy data is based on access control lists associated with input related to a user interface.

34. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein ~~the method further comprises~~ the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining a maximum penetration point.

35. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of accessing the security policy data and

the topology data related to a neighbor network device for which it has been determined that the packet could ~~be~~ reach.

36. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether ingress is allowed to a neighbor network device whose inbound interface for which it has been determined that the packet could ~~be~~ reach.

37. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet could reach.

38. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

39. (Currently Amended) An ~~system~~ apparatus as recited in Claim 38, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of recursively applying the step of determining whether there are any outbound interfaces.

40. (Canceled)

41 (Currently Amended) An ~~system~~ apparatus as recited in claim 27 wherein the packet parameters specify information corresponding to a plurality of packets.

42. (Currently Amended) An ~~system~~ apparatus as recited in claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

~~at~~ for a neighbor network device being represented as having been reached by the packet, determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress of the packet is permitted based on the static routing table.

43. (Currently Amended) An ~~system~~ apparatus of claim 42, ~~the method further comprising~~ wherein the one or more sequences of instructions further comprise instructions which,

when executed by the one or more processors, cause the one or more processors to perform the step of not ~~permitting~~ considering ~~egress through~~ any outbound interface through which egress of the packet is permitted by the static routing table[[,]] but not permitted by an access control list associated with the security policy data.

44. (Currently Amended) An ~~system~~ apparatus as recited in claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

~~at~~ for a neighbor network device for which it is determined that the packet could reach, determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface of the neighbor network device, representing an egress by the packet as part of the representing of the travel of the packet.

45. (Currently Amended) An ~~system~~ apparatus as recited in claim 27, ~~further comprises~~ wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving packet parameters that support transmission control protocol flags.

46. (Currently Amended) An ~~system~~ apparatus as recited in claim 27, wherein the results comprise a graphical display of at least allowed paths of the packet.

47. (Currently Amended) An ~~system~~ apparatus as recited in claim 27, wherein the graphical display also includes at least a mapping of network devices and connections between the network devices.

48. (Currently Amended) An ~~system~~ apparatus as recited in Claim 27, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of:

defining a packet flow by at least specifying a source address, a source port, and a destination port;

starting a loop for a current network device;

accessing the ACL data stored in an ACL database and the topology data stored in a topology database;

deciding whether an ingress interface of a current network device allows entry into the current network device,

if the entry is not permitted, then terminating a loop for the current network device,

if the entry is permitted continuing the loop;

determining if a static routing table is present,

if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and

if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces;

determining if there are any neighboring network devices,

if there are not any neighboring network devices, then

an indication of the current network device is returned, as results of the step of representing, as a maximum penetration point, and

the loop is terminated, and

if there is a neighboring network device, then the loop continues;

determining whether or not there are any remaining outbound interfaces that the packet has not reached,

if there are no more remaining outbound interfaces, then the loop is terminated, and

if there are more remaining interfaces, then the current network device is set to the neighboring network device corresponding one of the remaining outbound interfaces; and

if the loop has not been terminated for the current network device, restarting the loop for the current network device.

49. (Currently Amended) A computer-readable storage medium ~~carrying~~ storing one or more sequences of instructions that comprise instructions ~~for determining network penetration, wherein execution of the one or more sequences of instructions by one or more processors causes~~ which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

representing a possible travel of a packet in a network based on topology data and on security policy data; ~~and,~~

wherein the step of representing comprises:

checking an inbound access control list (ACL), included in the security policy

data, of an interface of a network device comprising a network entry point for the packet;

if the inbound ACL permits ingress of the packet, checking one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted;

for each of the one or more possible outbound interfaces on which the egress of the packet is permitted, repeating the checking steps with respect to each neighbor network device that is connected to each of the one or more possible outbound interfaces;

providing an output that specifies a possible penetration of the packet into the network, based on the step of representing.

50. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the security policy data comprises one or more access control lists of one or more network devices in the network.

51. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein ~~the instructions further comprise~~ the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving packet parameters.

52. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein the packet parameters comprise an entry point where the packet enters the

network.

53. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein the packet parameters comprise a destination address.

54. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein ~~the instructions further comprise~~ the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of reading topology information from a topology database.

55. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the topology data is based on input related to a user interface.

56. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the security policy data is based on access control lists associated with input related to a user interface.

57. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein ~~the instructions further comprise~~ the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining a maximum penetration point.

58. (Currently Amended) A computer-readable storage medium as recited in Claim 49,

wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of accessing the security policy data and the topology data related to a neighbor network device for which it has been determined that the packet could reach.

59. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether ingress is allowed to a neighbor network device whose inbound interface for which it has been determined that the packet could ~~be~~ reach.

60. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining whether there are any neighboring network devices to a neighbor network device for which it has been determined that the packet could ~~be~~ reach.

61. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of determining

whether there are any possible outbound interfaces that have not yet been checked for whether there is another network device connected thereto.

62. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of recursively applying the step of determining whether there are any outbound interfaces.

63. (Canceled)

64. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein ~~the instructions further comprise~~ the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving packet parameters specifying information corresponding to a plurality of packets.

65. (Currently Amended) A computer-readable storage medium as recited in Claim 49, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

~~at~~ for a neighbor network device that could be reached by the packet, determining if a static routing table is present; and

if the static routing table is present, then

accessing the static routing table, and

determining an outbound interface through which egress of the packet is permitted based on the static routing table.

66. (Currently Amended) A computer-readable storage medium of claim 65, ~~the method further comprising~~ wherein the one or more sequences of instructions further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of not ~~permitting~~ considering ~~egress through~~ any outbound interface through which egress of the packet is permitted by the static routing table[[,]] but is not permitted by an access control list associated with the security policy data.

67. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

~~at~~ for a neighbor network device that could be reached by the packet, determining if a static routing table is present; and

if the static routing table is not present, then for each outbound interface of the neighbor network device, representing an egress by the packet as part of the representing of the travel of the packet.

68. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein ~~the instructions further comprise~~ the one or more sequences of instructions

further comprise instructions which, when executed by the one or more processors, cause the one or more processors to perform the step of receiving packet parameters that support transmission control protocol flags.

69. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein the results comprise a graphical display of at least allowed paths of the packet.

70. (Currently Amended) A computer-readable storage medium as recited in Claim 69, wherein the graphical display also includes at least a mapping of network devices and connections between the network devices.

71. (Currently Amended) A computer-readable storage medium as recited in Claim 51, wherein the instructions that cause the one or more processors to perform the step of representing comprise[[s]] instructions which, when executed by the one or more processors, cause the one or more processors to perform the steps of:

defining a packet flow by at least specifying a source address, a source port, and a destination port;

starting a loop for a current network device;

accessing the ACL data stored in an ACL database and the topology data stored in a topology database;

deciding whether an ingress interface of a current network device allows entry into the current network device,

if the entry is not permitted, then terminating a loop for the current network device,

if the entry is permitted continuing the loop;

determining if a static routing table is present,

if the static routing table is present then determining to which interface outbound traffic is permitted to exit, and

if the static routing table is not present, then allowing outbound traffic to exit through all outbound interfaces;

determining if there are any neighboring network devices,

if there are not any neighboring network devices, then an indication of the current network device is returned as results of the step of simulation as a maximum penetration point, and the loop is terminated, and

if there is a neighboring network device, then the loop continues;

determining whether or not there are any remaining outbound interfaces that the packet has not reached,

if there are no more remaining outbound interfaces, then the loop is terminated, and

if there are more remaining interfaces, then the current network device is set to the neighboring network device corresponding one of the remaining outbound interfaces; and

if the loop has not been terminated for the current network device, restarting the loop for the current network device; and

the method further comprising the step of:

displaying the results of the simulating by at least displaying

an allowed packet path, if found, and

the maximum penetration point.

72. (Currently Amended) An ~~system~~ apparatus for determining network penetration comprising:

means for representing a possible travel of a packet in a network based on topology data and on security policy data; ~~and,~~

wherein the means for representing comprise:

means for checking an inbound access control list (ACL), included in the security policy data, of an interface of a network device comprising a network entry point for the packet;

means for checking one or more outbound ACLs for each outbound interface of the network device to determine one or more possible outbound interfaces on which egress of the packet is permitted when the inbound ACL permits ingress of the packet;

means for repeatedly invoking the means for checking the inbound ACL and the means for checking the one or more outbound ACLs with respect to each neighbor network device that is connected to each of the one or more possible outbound interfaces on which the egress of the packet is permitted;

means for providing an output that specifies a possible penetration of the packet into the network, based on ~~the step of~~ output from the means for representing.